

Normalization of Quaternionic Polynomials

Hongbo Li, Lei Huang, Yue Liu

KLMM, AMSS, Chinese Academy of Sciences, Beijing 100190, China

hli@mmrc.iss.ac.cn, lhuang@mmrc.iss.ac.cn, liuyue10@mails.gucas.ac.cn

ABSTRACT

Quaternionic polynomials are generated by quaternionic variables and the quaternionic product. This paper proposes the generating ideal of quaternionic polynomials in tensor algebra, finds the Gröbner base of the ideal in the case of pure imaginary quaternionic variables, and describes the normal forms of such quaternionic polynomials explicitly.

Categories and Subject Descriptors

I.1.1 [Computing Methodologies]: SYMBOLIC AND ALGEBRAIC MANIPULATION

General Terms

Theory

Keywords

Quaternionic polynomial ring; syzygy ideal; non-commutative Gröbner base; normal form; Clifford algebra.

1. INTRODUCTION

Quaternions are one of the simplest examples of a non-commutative associative algebra. When pure imaginary quaternions are used to represent 3D vectors, the adjoint action of the group of unit quaternions upon them provides a representation of all 3D rotations. Because of this, quaternions have important applications in 3D Euclidean computing [1].

In symbolic geometric computing, when geometric entities and their transformations are represented by coordinate-free symbols, algebraic manipulations among the symbols often lead to rather simple and geometrically interpretable results [3]. For example, using \mathbf{v} instead of $x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ as a vector variable, provides a typical coordinate-free representation of a 3D direction (or point) by a pure imaginary quaternion. Under the quaternionic product, these variables generate a ring of non-commutative polynomials. It is natural to ask

for symbolic algebraic algorithms to manipulate such *quaternionic polynomials*.

When the coefficients of the quaternionic polynomials are taken in the field of rational numbers \mathbb{Q} , the quaternionic product, being associative and multilinear, must be a quotient of the \mathbb{Q} -tensor product modulo an ideal \mathcal{I} whose generators are some tensors. Finding such generators and proving that they are sufficient to define the quaternionic product is the first task to finish. The first theorem in this paper provides very simple generators of \mathcal{I} , called the *syzygy ideal* of quaternionic polynomials.

The next task is naturally on computing the Gröbner bases of \mathcal{I} and then the normal forms of quaternionic polynomials. This can always be done using the classical theory and algorithm on non-commutative Gröbner bases [4]. For a fixed number n of quaternionic variables, one can compute a Gröbner base of the syzygy ideal \mathcal{I} in the n variables, and for every degree d , the number of degree- d polynomials in the computed Gröbner base is finite. After investigating the elements in the Gröbner bases for small values of n and d , we come up with some observations on the general form of the Gröbner base for arbitrary n and d , and of the normal forms of quaternionic polynomials with respect to the Gröbner base.

The main part of this paper is the establishment of two theorems that provide explicitly (1) a reduced Gröbner base of the syzygy ideal \mathcal{I} of quaternionic polynomials in n pure imaginary quaternionic variables, (2) the structure of the normal forms relative to the Gröbner base. The results are extremely simple. For example, each polynomial in the Gröbner base has either 2 or 4 terms; the sequence of variables in a monomial of normal form always forms two intertwining non-descending subsequences in terms of the ordering of the variables (Figure 1 and Figure 2 of this paper).

The proofs of the theorems are very long and are divided into many cases. We provide detailed proofs for several cases for illustration, but skip the rest by limitation of the size of this paper. The results in this paper are not only foundations for symbolic manipulations of quaternionic polynomials, but also helpful in exploring general results on the Clifford product among vectors of arbitrary dimension [2], now that the dimension-three case is solved here as a by-product.

2. QUATERNIONIC POLYNOMIAL RING GENERATED BY VECTORS

Let $\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n$ be a set of symbols representing quaternionic variables, and let $\bar{\mathbf{q}}_1, \bar{\mathbf{q}}_2, \dots, \bar{\mathbf{q}}_n$ be the corresponding quaternionic conjugates. A *vector* \mathbf{v} refers to a pure imagi-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 20XX ACM X-XXXXX-XX-X/XX/XX ...\$15.00.

nary quaternion, i.e., $\bar{\mathbf{v}} = -\mathbf{v}$, and a scalar \mathbf{s} refers to a real quaternion, i.e., $\bar{\mathbf{s}} = \mathbf{s}$.

A *monic quaternionic monomial* in variables $\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n$ refers to the quaternionic product of a permutation of the elements in a multiset of the $2n$ symbols $\{\mathbf{q}_i, \bar{\mathbf{q}}_i \mid i = 1, \dots, n\}$. A *quaternionic polynomial* with rational coefficients is a linear combination of monic quaternionic monomials with coefficients in the rational numbers field \mathbb{Q} . We always use juxtaposition of elements to represent their quaternionic product. For a monomial $\mathbf{Q} = \mathbf{q}_{i_1} \mathbf{q}_{i_2} \cdots \mathbf{q}_{i_k}$, its *reversion* is

$$\mathbf{Q}^\dagger := \mathbf{q}_{i_k} \cdots \mathbf{q}_{i_2} \mathbf{q}_{i_1}. \quad (2.1)$$

The quaternionic product is the quotient of the \mathbb{Q} -tensor product modulo some *syzygy ideal*. Since in symbolic manipulation, a scalar is characterized by its commutativity with everything, we first consider characterizing vectors and their quaternionic products by the syzygy ideal, then extend the results to general quaternionic variables.

Let $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ be vector variables. They belong to a 3D real inner-product space with metric $\text{diag}(-1, -1, -1)$. As the standard basis $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ cannot be constructed from the given vector variables without using square-root and division operations, they are not allowed in manipulating the quaternionic polynomials of the \mathbf{v}_i .

Let $\mathbf{v}_1 \prec \mathbf{v}_2 \cdots \prec \mathbf{v}_n$. For a monic quaternionic monomial $\mathbf{v}_{i_1} \mathbf{v}_{i_2} \cdots \mathbf{v}_{i_k}$, the *leading variable* refers to \mathbf{v}_{i_1} , and the *trailing variable* refers to \mathbf{v}_{i_k} . The monomial is said to be *non-descending* if $i_1 \leq i_2 \leq \dots \leq i_k$, and is said to be *ascending* if $i_1 < i_2 < \dots < i_k$. The *degree*, or *length*, of the monomial is k . The *degree* of a quaternionic polynomial is the biggest degree of its monomials disregarding the \mathbb{Q} -coefficients. The *lexicographic ordering* among monomials is always assumed. The *leading term* of a quaternionic polynomial is the term of highest order.

The *inner product* of two vectors (not necessarily vector variables) $\mathbf{v}_i, \mathbf{v}_j$ is defined by

$$[\mathbf{v}_i \mathbf{v}_j] := (\mathbf{v}_i \mathbf{v}_j + \mathbf{v}_j \mathbf{v}_i)/2. \quad (2.2)$$

The result is a scalar, so it commutes with a third vector \mathbf{v}_k : $[\mathbf{v}_i \mathbf{v}_j] \mathbf{v}_k = \mathbf{v}_k [\mathbf{v}_i \mathbf{v}_j]$.

The *vector product* of two vectors $\mathbf{v}_i, \mathbf{v}_j$ is defined by

$$\mathbf{v}_i \times \mathbf{v}_j := (\mathbf{v}_i \mathbf{v}_j - \mathbf{v}_j \mathbf{v}_i)/2. \quad (2.3)$$

The result is a vector, so its inner product with a third vector \mathbf{v}_k is a scalar. Define

$$[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] := (\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k - \mathbf{v}_k \mathbf{v}_j \mathbf{v}_i)/2. \quad (2.4)$$

Then $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] = [(\mathbf{v}_i \times \mathbf{v}_j) \mathbf{v}_k]$ is a scalar, so for a fourth vector \mathbf{v}_l , $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] \mathbf{v}_l = \mathbf{v}_l [\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$.

Define

$$[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k \mathbf{v}_l] := (\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k \mathbf{v}_l + \mathbf{v}_l \mathbf{v}_k \mathbf{v}_j \mathbf{v}_i)/2. \quad (2.5)$$

THEOREM 1. Let $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ be n different symbols, where $n \geq 2$. Define the product among them, denoted by juxtaposition of elements, as the \mathbb{Q} -tensor product modulo the two-sided ideal generated by the following tensors:

$$\begin{aligned} \text{V2: } & \mathbf{v}_i \otimes \mathbf{v}_i \otimes \mathbf{v}_j - \mathbf{v}_j \otimes \mathbf{v}_i \otimes \mathbf{v}_i; \\ \text{V3: } & (\mathbf{v}_i \otimes \mathbf{v}_j + \mathbf{v}_j \otimes \mathbf{v}_i) \otimes \mathbf{v}_k - \mathbf{v}_k \otimes (\mathbf{v}_i \otimes \mathbf{v}_j + \mathbf{v}_j \otimes \mathbf{v}_i); \\ \text{V4: } & (\mathbf{v}_i \otimes \mathbf{v}_j \otimes \mathbf{v}_k - \mathbf{v}_k \otimes \mathbf{v}_j \otimes \mathbf{v}_i) \otimes \mathbf{v}_l \\ & - \mathbf{v}_l \otimes (\mathbf{v}_i \otimes \mathbf{v}_j \otimes \mathbf{v}_k - \mathbf{v}_k \otimes \mathbf{v}_j \otimes \mathbf{v}_i), \end{aligned} \quad (2.6)$$

for any $i \neq j \neq k \neq l$ in $1, 2, \dots, n$. Denote by \mathcal{Q} the \mathbb{Q} -algebra defined by the above product and generated by the \mathbf{v}_i . Denote

$$\vec{\mathcal{Q}} := \mathbb{Q}(\{\mathbf{v}_i \otimes \mathbf{v}_l + \mathbf{v}_l \otimes \mathbf{v}_i, \mathbf{v}_i \otimes \mathbf{v}_j \otimes \mathbf{v}_k - \mathbf{v}_k \otimes \mathbf{v}_j \otimes \mathbf{v}_i \mid i \neq j \neq k\}). \quad (2.7)$$

Then (1) the \mathbf{v}_i and $\mathbf{v}_i \times \mathbf{v}_j$ span a 3D $\vec{\mathcal{Q}}$ -vector space \mathcal{V}^3 ; (2) if all the elements in (2.7) extending \mathbb{Q} are real numbers, and the inner product of real vector space \mathcal{V}^3 induced from (2.2) is definite, then the product among the \mathbf{v}_i is the quaternionic product, i.e., \mathcal{Q} is the quaternionic polynomial ring generated by the \mathbf{v}_i as vector variables.

Proof. The proof is composed of the following steps:

Step 1. For all $1 \leq i, j, k, l \leq n$,

$$\begin{aligned} \mathbf{v}_i \mathbf{v}_i \mathbf{v}_j &= \mathbf{v}_j \mathbf{v}_i \mathbf{v}_i; \\ (\mathbf{v}_i \mathbf{v}_j + \mathbf{v}_j \mathbf{v}_i) \mathbf{v}_k &= \mathbf{v}_k (\mathbf{v}_i \mathbf{v}_j + \mathbf{v}_j \mathbf{v}_i); \\ (\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k - \mathbf{v}_k \mathbf{v}_j \mathbf{v}_i) \mathbf{v}_l &= \mathbf{v}_l (\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k - \mathbf{v}_k \mathbf{v}_j \mathbf{v}_i). \end{aligned} \quad (2.8)$$

The proof is easily established by verifying that V3 for $i = k$, and V4 for $l = i$ or j are in the ideal generated by elements in (2.6). So the center of the ring \mathcal{Q} is the subring generated by the $[\mathbf{v}_i \mathbf{v}_i]$, $[\mathbf{v}_i \mathbf{v}_j]$, $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$ for all $1 \leq i < j < k \leq n$.

Obviously, the latter two equalities in (2.8) can be written as the following *shift invariance* of $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$ and $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k \mathbf{v}_l]$:

$$[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] = [\mathbf{v}_k \mathbf{v}_i \mathbf{v}_j], \quad [\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k \mathbf{v}_l] = [\mathbf{v}_l \mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]. \quad (2.9)$$

Step 2. Since $\mathbf{v}_i \otimes \mathbf{v}_i$, $\mathbf{v}_i \otimes \mathbf{v}_j + \mathbf{v}_j \otimes \mathbf{v}_i$ and $\mathbf{v}_i \otimes \mathbf{v}_j \otimes \mathbf{v}_k - \mathbf{v}_k \otimes \mathbf{v}_j \otimes \mathbf{v}_i$ for all $1 \leq i < j < k \leq n$ are not in the ideal generated by elements V2, V3, V4, $[\mathbf{v}_i \mathbf{v}_i]$, $[\mathbf{v}_i \mathbf{v}_j]$, $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$ for all $1 \leq i < j < k \leq n$ are nonzero.

Consider the following *Cramer's rule*: for all i, j, k, l ,

$$[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] \mathbf{v}_l - [\mathbf{v}_i \mathbf{v}_j \mathbf{v}_l] \mathbf{v}_k + [\mathbf{v}_i \mathbf{v}_k \mathbf{v}_l] \mathbf{v}_j - \mathbf{v}_i [\mathbf{v}_j \mathbf{v}_k \mathbf{v}_l] = 0. \quad (2.10)$$

By the first equality in (2.9), the left side of (2.10) can be simplified to $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] \mathbf{v}_l - \mathbf{v}_l [\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$, which equals zero by the last equality in (2.8). So if $n > 2$, the \mathbf{v}_i span a 3D $\vec{\mathcal{Q}}$ -vector space.

Step 3. The following relations can be verified using (2.8):

$$\begin{aligned} (\mathbf{v}_i \times \mathbf{v}_j) \times \mathbf{v}_k &= [\mathbf{v}_j \mathbf{v}_k] \mathbf{v}_i - [\mathbf{v}_i \mathbf{v}_k] \mathbf{v}_j; \\ [(\mathbf{v}_i \times \mathbf{v}_j)(\mathbf{v}_k \times \mathbf{v}_l)] &= [\mathbf{v}_i \mathbf{v}_l] [\mathbf{v}_j \mathbf{v}_k] - [\mathbf{v}_i \mathbf{v}_k] [\mathbf{v}_j \mathbf{v}_l]; \\ (\mathbf{v}_i \times \mathbf{v}_j) \times (\mathbf{v}_k \times \mathbf{v}_l) &= [\mathbf{v}_j \mathbf{v}_k \mathbf{v}_l] \mathbf{v}_i - [\mathbf{v}_i \mathbf{v}_k \mathbf{v}_l] \mathbf{v}_j. \end{aligned} \quad (2.11)$$

Notice that in the corresponding formulas for the vector algebra over \mathbb{R}^3 , the signs on the right side of (2.11) are opposite. In fact, the expressions in the three lines of (2.11) are respectively equal to

$$\frac{\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k - \mathbf{v}_k \mathbf{v}_i \mathbf{v}_j}{2}; \quad [\mathbf{v}_i \mathbf{v}_j (\mathbf{v}_k \times \mathbf{v}_l)]; \quad \frac{\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k \mathbf{v}_l - \mathbf{v}_k \mathbf{v}_l \mathbf{v}_i \mathbf{v}_j}{2}.$$

If $n = 2$, it is easy to see that $\mathbf{v}_1 \otimes \mathbf{v}_2 - \mathbf{v}_2 \otimes \mathbf{v}_1$, and $\mathbf{v}_1 \otimes \mathbf{v}_2 \otimes \mathbf{v}_1 \otimes \mathbf{v}_2 + \mathbf{v}_2 \otimes \mathbf{v}_1 \otimes \mathbf{v}_2 \otimes \mathbf{v}_1 - 2\mathbf{v}_1 \otimes \mathbf{v}_1 \otimes \mathbf{v}_2 \otimes \mathbf{v}_2$ are not in the defining ideal of \mathcal{Q} , so $\mathbf{v}_1 \times \mathbf{v}_2 \neq 0$, and

$$\begin{aligned} [(\mathbf{v}_1 \times \mathbf{v}_2) \mathbf{v}_1 \mathbf{v}_2] &= (\mathbf{v}_1 \times \mathbf{v}_2)(\mathbf{v}_1 \times \mathbf{v}_2) \\ &= (\mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_1 \mathbf{v}_2 + \mathbf{v}_2 \mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_1 - 2\mathbf{v}_1 \mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_2)/4 \\ &\neq 0. \end{aligned} \quad (2.12)$$

Then $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_1 \times \mathbf{v}_2$ are linearly independent over $\vec{\mathcal{Q}}$.

By (2.8) and (2.11), the following *Cramer's rule* can be verified: for all $1 \leq i, j, k, l, m \leq n$,

$$\begin{aligned} [(\mathbf{v}_i \times \mathbf{v}_j) \mathbf{v}_k \mathbf{v}_l] \mathbf{v}_m - [(\mathbf{v}_i \times \mathbf{v}_j) \mathbf{v}_k \mathbf{v}_m] \mathbf{v}_l \\ + [(\mathbf{v}_i \times \mathbf{v}_j) \mathbf{v}_l \mathbf{v}_m] \mathbf{v}_k - [\mathbf{v}_k \mathbf{v}_l \mathbf{v}_m] (\mathbf{v}_i \times \mathbf{v}_j) = 0. \end{aligned} \quad (2.13)$$

Hence the \mathbf{v}_i and $\mathbf{v}_j \times \mathbf{v}_k$ span a 3D $\vec{\mathbb{Q}}$ -vector space.

Step 4. The inner product defined by (2.2) can be extended bilinearly to all elements in \mathcal{V}^3 . Then $\mathbf{v}_1 \times \mathbf{v}_2$ is orthogonal to both \mathbf{v}_1 and \mathbf{v}_2 . Furthermore, the inner products of the three elements with themselves separately are all nonzero. When the $[\mathbf{v}_i \mathbf{v}_i]$, $[\mathbf{v}_i \mathbf{v}_j]$, $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$ are all real numbers, let

$$\mathbf{e}_1 = \mathbf{v}_1 / \sqrt{[\mathbf{v}_1 \mathbf{v}_1]}, \quad \mathbf{e}_2 = \mathbf{v}_1 \times \mathbf{v}_2 / \sqrt{[(\mathbf{v}_1 \times \mathbf{v}_2)(\mathbf{v}_1 \times \mathbf{v}_2)]},$$

and let $\mathbf{e}_3 = \mathbf{e}_1 \times \mathbf{e}_2$. Then $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ form an orthogonal basis of \mathcal{V}^3 , and $[\mathbf{e}_i \mathbf{e}_i] = \pm 1$. Furthermore, $\mathbf{e}_3^2 = [\mathbf{e}_3 \mathbf{e}_3] = -\mathbf{e}_1^2 \mathbf{e}_2^2$. So the metric of \mathcal{V}^3 is either $\text{diag}(-1, -1, -1)$ or $\text{diag}(-1, 1, 1)$.

Step 5. It is easy to prove $\mathbf{e}_2 \mathbf{e}_3 = \mathbf{e}_2 \times \mathbf{e}_3 = -\mathbf{e}_1^2 \mathbf{e}_1$ and $\mathbf{e}_3 \mathbf{e}_1 = \mathbf{e}_3 \times \mathbf{e}_1 = -\mathbf{e}_1^2 \mathbf{e}_2$. Moreover, $\mathbf{e}_1 \mathbf{e}_2 = \mathbf{e}_1 \times \mathbf{e}_2 = \mathbf{e}_3$. So if $\mathbf{e}_i^2 = -1$ for $i = 1, 2, 3$, then the product in \mathcal{V}^3 is the quaternionic product. \square

As a consequence, all polynomial identities among the \mathbf{v}_i in the ring \mathcal{Q} are generated by relations of the form $[\mathbf{v}_i \mathbf{v}_j] \mathbf{v}_k = \mathbf{v}_k [\mathbf{v}_i \mathbf{v}_j]$ and $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] \mathbf{v}_l = \mathbf{v}_l [\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$, or equivalently, by relations of the form $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] = [\mathbf{v}_k \mathbf{v}_i \mathbf{v}_j]$ and $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k \mathbf{v}_l] = [\mathbf{v}_l \mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$. Neither the assumption that the $[\mathbf{v}_i \mathbf{v}_i]$, $[\mathbf{v}_i \mathbf{v}_j]$ and $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$ are real numbers, nor the assumption that the metric of \mathcal{V}^3 is definite, can be represented by polynomial equalities of the \mathbf{v}_i .

Henceforth we refer to the ring \mathcal{Q} defined in Theorem 1 as the *quaternionic polynomial ring* generated by vector variables \mathbf{v}_i , and call the defining ideal of \mathcal{Q} the *syzygy ideal*, and denote it by $\mathcal{I}[\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n]$.

Let $\mathbf{V}_k = \mathbf{v}_{j_1} \mathbf{v}_{j_2} \cdots \mathbf{v}_{j_k}$. Define

$$[\mathbf{V}_k] := (\mathbf{V}_k + (-1)^k \mathbf{V}_k) / 2, \quad A(\mathbf{V}_k) := (\mathbf{V}_k - (-1)^k \mathbf{V}_k) / 2. \quad (2.14)$$

PROPOSITION 2. $\mathbf{v}_i [\mathbf{V}_k] - [\mathbf{V}_k] \mathbf{v}_i$ is in $\mathcal{I}[\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n]$. The commutation relation $\mathbf{v}_i [\mathbf{V}_k] = [\mathbf{V}_k] \mathbf{v}_i$ can also be written as the following shift-invariance:

$$[\mathbf{v}_i \mathbf{V}_k] = [\mathbf{V}_k \mathbf{v}_i]. \quad (2.15)$$

The $A(\mathbf{V}_k)$ are in the 3D $\vec{\mathbb{Q}}$ -vector space spanned by the \mathbf{v}_i and $\mathbf{v}_j \times \mathbf{v}_k$.

Proof. The following identities can be established by induction, although not very easy: for all $l > 1$,

$$\begin{aligned} [\mathbf{v}_{j_1} \mathbf{v}_{j_2} \cdots \mathbf{v}_{j_{2l}}] &= \sum_{i=2}^{2l} (-1)^i [\mathbf{v}_{j_1} \mathbf{v}_{j_i}] [\mathbf{v}_{j_2} \mathbf{v}_{j_3} \cdots \check{\mathbf{v}}_{j_i} \cdots \mathbf{v}_{j_{2l}}]; \\ A(\mathbf{V}_{2l-1}) &= \sum_{(2l-2,1) \vdash \mathbf{V}_{2l-1}} [\mathbf{V}_{2l+1(1)}] \mathbf{V}_{2l-1(2)}; \\ A(\mathbf{V}_{2l}) &= \sum_{(2l-2,2) \vdash \mathbf{V}_{2l}} [\mathbf{V}_{2l(1)}] A(\mathbf{V}_{2l(2)}); \\ [\mathbf{V}_{2l+1}] &= \sum_{(2l-2,3) \vdash \mathbf{V}_{2l+1}} [\mathbf{V}_{2l+1(1)}] [\mathbf{V}_{2l+1(2)}], \end{aligned} \quad (2.16)$$

where (i) $\check{\mathbf{v}}_{j_i}$ denotes that \mathbf{v}_{j_i} does not occur in the sequence, (ii) $(h, m-h) \vdash \mathbf{V}_m$ is a bipartition of the m elements in the sequence \mathbf{V}_m into two subsequences $\mathbf{V}_{m(1)}$ and $\mathbf{V}_{m(2)}$ of length h and $m-h$ respectively, (iii) in $[\mathbf{V}_{m(1)}]$, the product of the h elements in the subsequence is denoted by the same symbol $\mathbf{V}_{m(1)}$, (iv) the summation $\sum_{(h,m-h) \vdash \mathbf{V}_m}$ is over all such bipartitions of \mathbf{V}_m , and the sign of permutation of the new sequence $\mathbf{V}_{m(1)}, \mathbf{V}_{m(2)}$ is assumed to be carried by the first factor $[\mathbf{V}_{m(1)}]$ of the addend. All the conclusions of the proposition follow (2.16) and (2.8). \square

Alternatively, we can use existing results on Clifford algebras to deduce (2.16) directly. In the proof of Theorem

1, we have shown that the \mathbf{v}_i and $\mathbf{v}_j \times \mathbf{v}_k$ span a 3D $\vec{\mathbb{Q}}$ -vector space. To show the difference between the quaternionic product and the Clifford product among the vectors \mathbf{v}_i we need to reduce the field $\vec{\mathbb{Q}}$.

LEMMA 3. Let \mathcal{Q} be the \mathbb{Q} -algebra defined by (2.6). Then for vectors $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_6}$,

$$[\mathbf{v}_{i_1} \mathbf{v}_{i_2} \mathbf{v}_{i_3}] [\mathbf{v}_{i_4} \mathbf{v}_{i_5} \mathbf{v}_{i_6}] = - \begin{vmatrix} [\mathbf{v}_{i_1} \mathbf{v}_{i_4}] & [\mathbf{v}_{i_1} \mathbf{v}_{i_5}] & [\mathbf{v}_{i_1} \mathbf{v}_{i_6}] \\ [\mathbf{v}_{i_2} \mathbf{v}_{i_4}] & [\mathbf{v}_{i_2} \mathbf{v}_{i_5}] & [\mathbf{v}_{i_2} \mathbf{v}_{i_6}] \\ [\mathbf{v}_{i_3} \mathbf{v}_{i_4}] & [\mathbf{v}_{i_3} \mathbf{v}_{i_5}] & [\mathbf{v}_{i_3} \mathbf{v}_{i_6}] \end{vmatrix}. \quad (2.17)$$

Proof. Using the second equality of (2.11) in the reverse direction, we can write the right side of (2.17) after expanding the determinant as

$$\begin{aligned} & -[\mathbf{v}_{i_1} \mathbf{v}_{i_4}] [(\mathbf{v}_{i_2} \times \mathbf{v}_{i_3})(\mathbf{v}_{i_5} \times \mathbf{v}_{i_6})] \\ & + [\mathbf{v}_{i_2} \mathbf{v}_{i_4}] [(\mathbf{v}_{i_1} \times \mathbf{v}_{i_3})(\mathbf{v}_{i_5} \times \mathbf{v}_{i_6})] \\ & - [\mathbf{v}_{i_3} \mathbf{v}_{i_4}] [(\mathbf{v}_{i_1} \times \mathbf{v}_{i_2})(\mathbf{v}_{i_5} \times \mathbf{v}_{i_6})] \\ & = -\{[\mathbf{v}_{i_2} \mathbf{v}_{i_3}(\mathbf{v}_{i_5} \times \mathbf{v}_{i_6})] \mathbf{v}_{i_1} - [\mathbf{v}_{i_1} \mathbf{v}_{i_3}(\mathbf{v}_{i_5} \times \mathbf{v}_{i_6})] \mathbf{v}_{i_2} \\ & \quad + [\mathbf{v}_{i_1} \mathbf{v}_{i_2}(\mathbf{v}_{i_5} \times \mathbf{v}_{i_6})] \mathbf{v}_{i_3}\} \mathbf{v}_{i_4}. \end{aligned}$$

By (2.13), the above expression can be simplified to $-\mathbf{v}_{i_1} \mathbf{v}_{i_2} \mathbf{v}_{i_3} [(\mathbf{v}_{i_5} \times \mathbf{v}_{i_6}) \mathbf{v}_{i_4}]$, which equals the left side of (2.17). \square

Let

$$\hat{\mathbb{Q}} := \mathbb{Q}(\{\mathbf{v}_i \otimes \mathbf{v}_l + \mathbf{v}_l \otimes \mathbf{v}_i, | 1 \leq i, l \leq n\}). \quad (2.18)$$

Then when $n = 2$, by (2.12), $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_1 \times \mathbf{v}_2$ span a 3D inner-product space over $\hat{\mathbb{Q}}$. When $n > 2$, let

$$\iota := [\mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_3]. \quad (2.19)$$

Then $\iota \neq 0$, and $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] = \iota \{(\iota [\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]) / (\iota)\} \in \hat{\mathbb{Q}} \iota$. The center of \mathcal{Q} as a $\hat{\mathbb{Q}}$ -algebra is $\hat{\mathbb{Q}} + \hat{\mathbb{Q}} \iota$.

By multiplying (2.10) with ι , we get that the \mathbf{v}_i span a 3D $\hat{\mathbb{Q}}$ -vector space $\hat{\mathcal{V}}^3$. Furthermore, from (2.13) we get that the $\iota \mathbf{v}_i \times \mathbf{v}_j$ are in $\hat{\mathcal{V}}^3$. The inner product between the \mathbf{v}_i can be extended bilinearly to an inner product in $\hat{\mathcal{V}}^3$.

In the \mathbb{Q} -Clifford algebra $Cl(\hat{\mathcal{V}}^3)$ over $\hat{\mathcal{V}}^3$, By Theorem 5.64, Theorem 5.65 and Proposition 6.22 in [3], the two sides of the four equalities in (2.16) are different expressions of the grade-0,1,2,3 part of $\mathbf{V}_{2l}, \mathbf{V}_{2l-1}, \mathbf{V}_{2l}, \mathbf{V}_{2l+1}$ respectively. In $Cl(\hat{\mathcal{V}}^3)$, ι is not a scalar, but a grade-3 element. In the case of quaternions, the quaternionic product is a homomorphic image of the Clifford product because of V2, V3, so (2.16) is automatically satisfied.

The right side of the third equality in (2.16) when multiplied by ι , becomes a vector in $\hat{\mathcal{V}}^3$, while the right side of the last equality when multiplied by ι , becomes an element in $\hat{\mathbb{Q}}$. These discussions lead to the following conclusion:

PROPOSITION 4. In the \mathbb{Q} -algebra \mathcal{Q} defined by (2.6), the \mathbf{v}_i and $\iota \mathbf{v}_i \times \mathbf{v}_j$ span a 3D $\hat{\mathbb{Q}}$ -vector space $\hat{\mathcal{V}}^3$. For any $k \geq 1$, $A(\mathbf{v}_{j_1} \mathbf{v}_{j_2} \cdots \mathbf{v}_{j_{2k+1}})$ and $\iota A(\mathbf{v}_{j_1} \mathbf{v}_{j_2} \cdots \mathbf{v}_{j_{2k}})$ are both in $\hat{\mathcal{V}}^3$.

Remark. In Clifford algebra, by Proposition 6.23 of [3], the outer product (or exterior product) of four vectors $\mathbf{v}_i, \mathbf{v}_j, \mathbf{v}_k, \mathbf{v}_l$ equals one quarter of V4. So when the field is extended to $\hat{\mathbb{Q}}$, V4 states that the dimension of the $\hat{\mathbb{Q}}$ -vector space spanned by the \mathbf{v}_m is at most three. From this aspect, V2, V3, V4 also generate the *syzygy ideal* of $Cl(\hat{\mathcal{V}}^3)$, if the latter is taken as a \mathbb{Q} -algebra.

3. QUATERNIONIC POLYNOMIAL RING

Let $\mathbf{q}_1, \dots, \mathbf{q}_n$ be quaternionic variables, and let $\bar{\mathbf{q}}_1, \dots, \bar{\mathbf{q}}_n$ be their quaternionic conjugates. To simplify notation, we introduce \mathbf{p}_i to represent any of $\mathbf{q}_i, \bar{\mathbf{q}}_i$, and define $\bar{\bar{\mathbf{q}}}_i := \mathbf{q}_i$. For a monomial $\mathbf{Q} = \mathbf{p}_{i_1} \cdots \mathbf{p}_{i_k}$, its *conjugate* is defined by

$$\bar{\mathbf{Q}} := \bar{\mathbf{p}}_{i_k} \cdots \bar{\mathbf{p}}_{i_2} \bar{\mathbf{p}}_{i_1}. \quad (3.1)$$

Define the *scalar part* $[\mathbf{Q}]$ and the *vector part* $A(\mathbf{Q})$ of \mathbf{Q} as following:

$$[\mathbf{Q}] := (\mathbf{Q} + \bar{\mathbf{Q}})/2, \quad A(\mathbf{Q}) := (\mathbf{Q} - \bar{\mathbf{Q}})/2. \quad (3.2)$$

Then $[\mathbf{q}_i]$ commutes with \mathbf{p}_j , and the quaternionic product among vectors $\mathbf{v}_i := A(\mathbf{q}_i)$ is characterized by (2.6). From Theorem 1 and Proposition 2 we can deduce the following:

THEOREM 5. *Let $\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n$ and $\bar{\mathbf{q}}_1, \bar{\mathbf{q}}_2, \dots, \bar{\mathbf{q}}_n$ be $2n$ different symbols, where $n \geq 2$. Let \mathbf{p}_i be one of $\mathbf{q}_i, \bar{\mathbf{q}}_i$, and let $\bar{\bar{\mathbf{q}}}_i = \mathbf{q}_i$. Define the product among the $2n$ symbols, denoted by juxtaposition of elements, as the \mathbb{Q} -tensor product modulo the two-sided ideal generated by the following tensors:*

$$\begin{aligned} \mathbf{Q0} &: \mathbf{q}_i \otimes \bar{\mathbf{q}}_i - \bar{\mathbf{q}}_i \otimes \mathbf{q}_i; \\ \mathbf{Q1} &: (\mathbf{q}_i + \bar{\mathbf{q}}_i) \otimes \mathbf{p}_j - \mathbf{p}_j \otimes (\mathbf{q}_i + \bar{\mathbf{q}}_i); \\ \mathbf{Q2} &: \mathbf{q}_i \otimes \bar{\mathbf{q}}_i \otimes \mathbf{p}_j - \mathbf{p}_j \otimes \mathbf{q}_i \otimes \bar{\mathbf{q}}_i; \\ \mathbf{Q3} &: (\mathbf{p}_i \otimes \mathbf{p}_j + \bar{\mathbf{p}}_j \otimes \bar{\mathbf{p}}_i) \otimes \mathbf{p}_k - \mathbf{p}_k \otimes (\mathbf{p}_i \otimes \mathbf{p}_j + \bar{\mathbf{p}}_j \otimes \bar{\mathbf{p}}_i); \\ \mathbf{Q4} &: (\mathbf{p}_i \otimes \mathbf{p}_j \otimes \mathbf{p}_k + \bar{\mathbf{p}}_k \otimes \bar{\mathbf{p}}_j \otimes \bar{\mathbf{p}}_i) \otimes \mathbf{p}_l \\ &\quad - \mathbf{p}_l \otimes (\mathbf{p}_i \otimes \mathbf{p}_j \otimes \mathbf{p}_k + \bar{\mathbf{p}}_k \otimes \bar{\mathbf{p}}_j \otimes \bar{\mathbf{p}}_i), \end{aligned} \quad (3.3)$$

for any $i \neq j \neq k \neq l$ in $1, 2, \dots, n$. Denote by $\tilde{\mathcal{Q}}$ the ring defined by the above product and generated by the \mathbf{p}_i , and denote

$$\tilde{\mathcal{Q}} := \mathbb{Q}(\{\mathbf{q}_i + \bar{\mathbf{q}}_i, \mathbf{q}_i \otimes \bar{\mathbf{q}}_i, \mathbf{p}_i \otimes \mathbf{p}_j + \bar{\mathbf{p}}_j \otimes \bar{\mathbf{p}}_i, \mathbf{p}_i \otimes \mathbf{p}_j \otimes \mathbf{p}_k + \bar{\mathbf{p}}_k \otimes \bar{\mathbf{p}}_j \otimes \bar{\mathbf{p}}_i \mid i \neq j \neq k\}). \quad (3.4)$$

Then (1) the $A(\mathbf{q}_i)$ and $A(\mathbf{q}_i) \times A(\mathbf{q}_j)$ span a $3D$ $\tilde{\mathcal{Q}}$ -vector space $\tilde{\mathcal{V}}^3$;

(2) if all the elements in (3.4) extending \mathbb{Q} are real numbers, and the inner product of real vector space $\tilde{\mathcal{V}}^3$ induced from (2.2) for the $\mathbf{v}_i = A(\mathbf{q}_i)$ is definite, then the product among the \mathbf{p}_i is the quaternionic product, with $\bar{\mathbf{q}}_i$ as the quaternionic conjugate of \mathbf{q}_i , i.e., $\tilde{\mathcal{Q}}$ is the quaternionic polynomial ring generated by the quaternionic variables \mathbf{q}_i .

Similarly, we refer to the ring $\tilde{\mathcal{Q}}$ defined in Theorem 5 as the *quaternionic polynomial ring* generated by quaternionic variables \mathbf{q}_i , and call the defining ideal of $\tilde{\mathcal{Q}}$ the *syzygy ideal*, and denote it by $\tilde{\mathcal{I}}[\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n]$.

PROPOSITION 6. *For all $k > 1$, let $\mathbf{Q} = \mathbf{p}_{i_1} \mathbf{p}_{i_2} \cdots \mathbf{p}_{i_k}$. Then $\mathbf{p}_j[\mathbf{Q}] - [\mathbf{Q}]\mathbf{p}_j$ is in the syzygy ideal $\tilde{\mathcal{I}}[\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n]$. $[\mathbf{p}_j \mathbf{Q}] - [\mathbf{Q} \mathbf{p}_j]$ is also in the syzygy ideal, and $A(\mathbf{Q})$ is in the $3D$ \mathbb{Q} -vector space $\tilde{\mathcal{V}}^3$.*

4. GRÖBNER BASE AND NORMAL FORM: MULTILINEAR CASE FOR VECTORS

Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ be vector variables. For two quaternionic monomials h_1, h_2 in the variables, h_1 is said to be *reduced* with respect to h_2 , if h_1 is not a *multiplier* of h_2 , or h_2 is not a *factor* of h_1 , i.e., there do not exist monomials l, r , including rational numbers, such that $h_1 = lh_2r$. For two quaternionic polynomials f and g , f is said to be *reduced*

with respect to g , if the leading term of f is reduced with respect to that of g . The term “*non-reduced*” means the opposite.

Let $\{f_1, f_2, \dots, f_k\}$ be a set of quaternionic polynomials. A set of quaternionic polynomials $\{g_1, g_2, \dots, g_m\}$ is said to be a *reduced Gröbner base* of the ideal $\mathcal{I} := \langle f_1, f_2, \dots, f_k \rangle$ generated by the f_i in the quaternionic polynomial ring, if (1) $\langle g_1, \dots, g_m \rangle = \mathcal{I}$, (2) the leading term of any element in \mathcal{I} is a multiplier of the leading term of some g_i , (3) the g_i are pairwise reduced with respect to each other.

The *reduction* of a polynomial f with respect to a reduced Gröbner base g_1, g_2, \dots, g_m is the repetitive procedure of dividing the first non-reduced term L of f by some g_i whose leading term is a factor of L , then updating f by replacing L with its remainder, until all terms of f are reduced. The result is called the *normal form* of f with respect to the Gröbner base.

By the classical theory of non-commutative Gröbner base [4], a reduced Gröbner base always exists for the syzygy ideal of quaternionic polynomials. However, the Gröbner base can be computed by computers only for small values of n (number of variables) and d (degree of polynomials in the Gröbner base). Our goal is to find the general form of the Gröbner base for arbitrary n which can even be a symbol. We first consider the multilinear case.

In a *multilinear monomial*, every variable occurs at most once. A *multilinear polynomial* is the sum of multilinear monomials with rational coefficients, where for every variable, its degree is the same in different monomials. The *multilinear product* is defined for two multilinear polynomials only when they do not have any common variable. The *multilinear addition* is defined only for multilinear polynomials having the same set of variables. All multilinear polynomials together with the multilinear product and multilinear addition form an algebraic system, called the *multilinear ring*. All monic multilinear monomials together with the multilinear product form another algebraic system, called the *multilinear monoid*.

An *ideal* of a multilinear ring or multilinear monoid is defined just as in the usual tensor-product case. The concepts of *reduced Gröbner base*, *reduction* and *normal form* have similar definitions, the theory and algorithm of non-commutative Gröbner base in [4] are still valid.

For example, for $m \leq n$ vector variables $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_m}$, the *multilinear quaternionic polynomial ring* $\mathcal{Q}^M[\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_m}]$ is composed of all multilinear quaternionic polynomials whose variables are among the \mathbf{v}_{i_k} , including polynomials of degree 0. The syzygy ideal $\mathcal{I}^M[\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_m}]$ of the ring is generated by elements of the form $[\mathbf{v}_{i_a} \mathbf{v}_{i_b}] \mathbf{v}_{i_c} - \mathbf{v}_{i_c} [\mathbf{v}_{i_a} \mathbf{v}_{i_b}]$ or $[\mathbf{v}_{i_a} \mathbf{v}_{i_b} \mathbf{v}_{i_c}] \mathbf{v}_{i_d} - \mathbf{v}_{i_d} [\mathbf{v}_{i_a} \mathbf{v}_{i_b} \mathbf{v}_{i_c}]$ for all $i_a \neq i_b \neq i_c \neq i_d$. The Gröbner base of the syzygy ideal is denoted by $\mathcal{G}^M[\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_m}]$.

When the variables $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_m}$ are replaced by another sequence $\mathbf{v}_{j_1}, \dots, \mathbf{v}_{j_m}$, the syzygy ideal of $\mathcal{Q}^M[\mathbf{v}_{j_1}, \dots, \mathbf{v}_{j_m}]$, and the Gröbner base of the syzygy ideal are obtained from those of $\mathcal{Q}^M[\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_m}]$ simply by a replacement of variables. From this aspect, what is important is the number m of variables, not the specific sequence of variables. We introduce \mathcal{Q}_m^M , \mathcal{I}_m^M , and \mathcal{G}_m^M to denote the multilinear quaternionic ring, its syzygy ideal, and the Gröbner base of the syzygy ideal, in m *unspecified vector variables*.

Notice that if \mathcal{G}_m^M is reduced, then it is a subset of a reduced Gröbner base of \mathcal{I}_m^M , as any polynomial of degree $\leq m$ in

\mathcal{I}_n^M is also in \mathcal{I}_m^M .

THEOREM 7. Let $\mathcal{I}^M[\mathbf{v}_1, \dots, \mathbf{v}_n]$ be the syzygy ideal of the multilinear ring $\mathcal{Q}^M[\mathbf{v}_1, \dots, \mathbf{v}_n]$ of multilinear quaternionic polynomials in n vector variables $\mathbf{v}_1 \prec \mathbf{v}_2 \prec \dots \prec \mathbf{v}_n$.

(1) [Gröbner base] The following are a reduced Gröbner base of $\mathcal{I}^M[\mathbf{v}_1, \dots, \mathbf{v}_n]$: for all $1 \leq i_1 < i_2 < \dots < i_m \leq n$,

$$\text{G3: } [\mathbf{v}_{i_3} \mathbf{v}_{i_2} \mathbf{v}_{i_1}] - [\mathbf{v}_{i_1} \mathbf{v}_{i_3} \mathbf{v}_{i_2}], \text{ and } [\mathbf{v}_{i_3} \mathbf{v}_{i_1} \mathbf{v}_{i_2}] - [\mathbf{v}_{i_2} \mathbf{v}_{i_3} \mathbf{v}_{i_1}];$$

$$\text{Gm: } [\mathbf{v}_{i_3} \mathbf{v}_{i_2} \mathbf{V} \mathbf{v}_{i_1}] - [\mathbf{v}_{i_2} \mathbf{V} \mathbf{v}_{i_1} \mathbf{v}_{i_3}], \text{ where } \mathbf{V} = \mathbf{v}_{i_4} \mathbf{v}_{i_5} \dots \mathbf{v}_{i_m}, \text{ and } 4 \leq m \leq n.$$

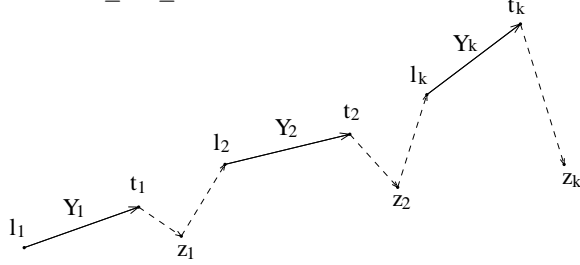


Figure 1: Double-ascending structure of a multilinear quaternionic monomial in normal form, where only the subscripts of vector variables are shown.

(2) [Normal form, see Figure 1] In a normal form, every term is up to coefficient of the form $\mathbf{V}_{Y_1} \mathbf{v}_{z_1} \mathbf{V}_{Y_2} \mathbf{v}_{z_2} \dots \mathbf{V}_{Y_k} \mathbf{v}_{z_k}$ or $\mathbf{V}_{Y_1} \mathbf{v}_{z_1} \dots \mathbf{V}_{Y_k} \mathbf{v}_{z_k} \mathbf{V}_{Y_{k+1}}$, where

- (i) $k \geq 0$,
- (ii) $\mathbf{v}_{z_1} \mathbf{v}_{z_2} \dots \mathbf{v}_{z_k}$ is ascending,
- (iii) every \mathbf{V}_{Y_i} is an ascending monomial of length ≥ 1 ,
- (iv) $\mathbf{V}_{Y_1} \mathbf{V}_{Y_2} \dots \mathbf{V}_{Y_k}$ (or $\mathbf{V}_{Y_1} \mathbf{V}_{Y_2} \dots \mathbf{V}_{Y_{k+1}}$ if $\mathbf{V}_{Y_{k+1}}$ occurs) is ascending,
- (v) for every $i \leq k$, if \mathbf{v}_{t_i} is the trailing variable of monomial \mathbf{V}_{Y_i} , then $\mathbf{v}_{z_i} \prec \mathbf{v}_{t_i}$.

Remark. In a normal form, as shown in Figure 1, although \mathbf{v}_{z_i} is lower than the trailing variable \mathbf{v}_{t_i} of \mathbf{V}_{Y_i} , it is allowed that the order of \mathbf{v}_{z_i} be at anywhere from above $\mathbf{v}_{z_{i-1}}$ up to below \mathbf{v}_{t_i} , and both $\mathbf{v}_{z_i} \prec \mathbf{v}_y$ and $\mathbf{v}_{z_i} \succ \mathbf{v}_y$ are possible for any variable $\mathbf{v}_y \neq \mathbf{v}_{t_i}$ in \mathbf{V}_{Y_j} where $j \leq i$.

Before proving the theorem, we introduce the following convenient term: let l_f, l_g be the leading terms of polynomials f, g respectively, if l_f equals l_g up to coefficient, then f, g are said to have *leading like terms*.

Proof. Observe that in the sequence G3, Gm for $m \geq 4$, the leading terms are pairwise reduced with respect to each other. The proof of the theorem is by induction, and is composed of many steps:

Step 1. G3, Gm for $m > 3$ generate the ideal \mathcal{I}_n^M . The proof is the following. By Proposition 2, G3, Gm are in the ideal. It is easy to show that for all $i \neq j \neq k \neq l$, $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k] - [\mathbf{v}_k \mathbf{v}_i \mathbf{v}_j]$ is reduced to zero by G3, and $[\mathbf{v}_i \mathbf{v}_j \mathbf{v}_k \mathbf{v}_l] - [\mathbf{v}_l \mathbf{v}_i \mathbf{v}_j \mathbf{v}_k]$ is reduced to G4 up to sign by G3. So all the generators of \mathcal{I}_n^M are in the ideal generated by G3, G4.

Step 2. The theorem obviously holds for $n = 3$. For $n = 4$, in Step 1 it is shown that for any $f \in \mathcal{I}_4^M$,

$$f = \sum_{\alpha} \lambda_{\alpha} \mathbf{v}_{\alpha} \text{G3} + \sum_{\beta} \lambda_{\beta} \text{G3 } \mathbf{v}_{\beta} + \lambda \text{G4}, \quad (4.1)$$

where G3 stands for a polynomial of type G3, and the λ 's are rational numbers. Notice that the leading variable of G3 is always \mathbf{v}_3 or \mathbf{v}_4 .

Assume that the leading term of f is reduced with respect to G3, G4. Further assume that before cancelling like terms on the right side of (4.1), the leading term is $\tilde{L} = \mathbf{v}_{i_1} \mathbf{v}_{i_2} \mathbf{v}_{i_3} \mathbf{v}_{i_4}$ up to coefficient. Then \tilde{L} is not reduced with respect to G3, G4, so it must be cancelled by other leading terms of the addends on the right side of (4.1). The following observations on (4.1) are obvious:

(i) If \tilde{L} comes from λG4 , i.e., equals $\mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_1$, then it is not the leading like term of either $\lambda_{\alpha} \mathbf{v}_{\alpha} \text{G3}$ or $\lambda_{\beta} \text{G3 } \mathbf{v}_{\beta}$. So \tilde{L} cannot come from λG4 .

(ii) If \tilde{L} comes from some $\lambda_i \mathbf{v}_i \text{G3}$, then it is not the leading like term of any other $\lambda_j \mathbf{v}_j \text{G3}$, so it has to be the leading like term of a unique $\lambda_k \text{G3 } \mathbf{v}_k$. Conversely, if \tilde{L} comes from some $\lambda_k \text{G3 } \mathbf{v}_k$, then it has to be the leading like term of a unique $\lambda_i \mathbf{v}_i \text{G3}$.

Based on the above two observations, we get that in $\tilde{L} = \mathbf{v}_{i_1} \mathbf{v}_{i_2} \mathbf{v}_{i_3} \mathbf{v}_{i_4}$, $\mathbf{v}_{i_1} \succ \mathbf{v}_{i_2} \succ \mathbf{v}_{i_3}$ and $\mathbf{v}_{i_2} \succ \mathbf{v}_{i_4}$. So either $\tilde{L} = \mathbf{v}_4 \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_1$ or $\tilde{L} = \mathbf{v}_4 \mathbf{v}_3 \mathbf{v}_1 \mathbf{v}_2$.

Step 3. For $n = 4$, we have the following conclusion:

$$\mathbf{v}_4 \text{G3} = \sum_{i=1}^3 \lambda_i \mathbf{v}_i \text{G3} + \sum_{j=1}^4 \lambda_j \text{G3 } \mathbf{v}_j. \quad (4.2)$$

To prove this we consider only $h = \mathbf{v}_4(\mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_1 - \mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_3 - \mathbf{v}_1 \mathbf{v}_3 \mathbf{v}_2 + \mathbf{v}_2 \mathbf{v}_3 \mathbf{v}_1)$. If (4.2) holds for $\mathbf{v}_4 \text{G3} = h$, then by interchanging subscripts 1,2, the right side of (4.2) keeps the same form.

$$\begin{aligned} h &= \underline{\mathbf{v}_4 \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_1} - \underline{\mathbf{v}_4 \mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_3} - \underline{\mathbf{v}_4 \mathbf{v}_1 \mathbf{v}_3 \mathbf{v}_2} + \underline{\mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_3 \mathbf{v}_1} \\ &\stackrel{\text{G3 } \mathbf{v}_j}{=} \underline{\mathbf{v}_2 \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_1} - \underline{\mathbf{v}_2 \mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_3} - \underline{\mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_1 \mathbf{v}_3} + \underline{\mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_3} \\ &\quad - \underline{\mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_1 \mathbf{v}_2} - \underline{\mathbf{v}_3 \mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_2} + \underline{\mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_3 \mathbf{v}_2} + \underline{\mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_1} \\ &\stackrel{\mathbf{v}_i \text{G3}, i < 4}{=} -\underline{\mathbf{v}_2 \mathbf{v}_3 \mathbf{v}_1 \mathbf{v}_4} + \underline{\mathbf{v}_1 \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4} + \underline{\mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_3 \mathbf{v}_4} - \underline{\mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_1 \mathbf{v}_4} \\ &\stackrel{\text{G3 } \mathbf{v}_4}{=} 0. \end{aligned}$$

The underlines give hint on the category of Gröbner base elements to be used in reduction.

Step 4. By (4.2), (4.1) can be rewritten as

$$f = \sum_{i < 4} \lambda_i \mathbf{v}_i \text{G3} + \sum_j \lambda_j \text{G3 } \mathbf{v}_j + \lambda \text{G4}. \quad (4.3)$$

By the analysis in Step 2, the leading term on the right side of (4.3) before cancelling like terms remains the leading term after cancelling like terms, violating the assumption that the leading term of f is reduced with respect to G3, G4. This proves that G3, G4 form a Gröbner base of \mathcal{I}_4^M .

Step 5. Let $T = \mathbf{v}_{i_1} \mathbf{v}_{i_2} \mathbf{v}_{i_3} \mathbf{v}_{i_4}$ be a term in the normal form of a degree-4 polynomial. By reduction with G3, if $i_j > i_{j+1}$ then $i_{j+2} > i_j$ is mandatory. So the sequence of subscripts must be one of $Y_1, Y_1 z_1, Y_1 z_1 Y_2$, and $Y_1 z_1 Y_2 z_2$, where z_i is a single subscript, each Y_i is an ascending sequence of subscripts, all the Y_i form a big ascending sequence of subscripts, and z_i is smaller than the trailing subscript of Y_i . If $z_1 > z_2$, then it must be that $T = \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_1$, which is not reduced with respect to G4. So $z_1 < z_2$. This proves the theorem for $n = 4$.

Step 6. Assume that the theorem holds for all $n < q$, where $q \geq 5$. When $n = q$, let $f \in \mathcal{I}_q^M$ and assume that its leading term is reduced with respect to G3, Gm for m up to q . By induction hypothesis, the degree of f must be q . We need to prove that f does not exist.

Since the generators of \mathcal{I}_q^M all have degree $< q$, it must

be that

$$f = \sum_{\alpha} \lambda_{\alpha} \mathbf{v}_{\alpha} f_{\alpha} + \sum_{\beta} \lambda_{\beta} f_{\beta} \mathbf{v}_{\beta}, \quad (4.4)$$

where the λ 's are coefficients, and $f_{\alpha}, f_{\beta} \in \mathcal{I}_{q-1}^M$ are of degree $q-1$. We do reduction to f_{α} with respect to the Gröbner base G3, Gm for m up to $q-1$ in the following special way: to every term T_i of f_{α} , let $T_i = \mu_i \mathbf{V}_i \mathbf{v}_{\alpha_i}$ where \mathbf{V}_i is a monomial of degree $q-2 \geq 3$ and μ_i is the coefficient, do reduction to monomial \mathbf{V}_i by Gröbner base G3, Gm for m up to $q-2$. After the reduction to every \mathbf{V}_i , $f_{\alpha} = \sum_j \lambda_j g_j \mathbf{v}_j + \tilde{f}_{\alpha}$, where $g_j \in \mathcal{I}_{q-2}^M$, and $\tilde{f}_{\alpha} \in \mathcal{I}_{q-1}^M$. Every term of \tilde{f}_{α} after removing its trailing variable is in normal form.

Now do reduction to \tilde{f}_{α} by G3, Gm for m up to $q-1$. Then $\tilde{f}_{\alpha} = \sum_{m < q} (\sum_{\alpha_m} \lambda_{\alpha_m} a_{\alpha_m} Gm + \lambda_{\beta_m} b_{\beta_m} Gm c_{\beta_m} + \sum_{\gamma_m} \lambda_{\gamma_m} Gm d_{\gamma_m})$, where a, b, c, d are monomials of degree ≥ 1 . The leading term of \tilde{f}_{α} must be the leading term of a unique $\lambda_{\alpha_m} a_{\alpha_m} Gm$, because it can only be non-reduced with respect to such a polynomial. Now substitute the above expressions of \tilde{f}_{α} , f_{α} into (4.4), and regroup the terms. We finally get

$$f = s + t, \text{ where } s = \sum_{m < q} \sum_{\alpha_m} \lambda_{\alpha_m} \mathbf{V}_{\alpha_m} Gm, \quad t = \sum_{\beta} \lambda_{\beta} h_{\beta} \mathbf{v}_{\beta}, \quad (4.5)$$

and where \mathbf{V}_{α_m} is a monomial of length $q-m$, $h_{\beta} \in \mathcal{I}_{q-1}^M$, with the following properties:

(a) If the leading term T_s of an addend $\lambda_{\alpha_m} \mathbf{V}_{\alpha_m} Gm$ is of the highest order among all leading terms in the addends of s , then T_s must be the leading term of s , and has no leading like term in any other addend of s .

(b) Furthermore, when $\mathbf{V}_{\alpha_m} = \mathbf{v}_{i_1} \mathbf{v}_{i_2} \cdots \mathbf{v}_{i_{q-m}}$ and the leading term of Gm is $\mathbf{v}_{j_1} \mathbf{v}_{j_2} \cdots \mathbf{v}_{j_m}$, then the degree- $(q-2)$ factor $\mathbf{v}_{i_2} \cdots \mathbf{v}_{i_{q-m}} \mathbf{v}_{j_1} \mathbf{v}_{j_2} \cdots \mathbf{v}_{j_{m-1}}$ of T_s is in normal form.

Step 7. In (4.5), the leading term T_s of s comes from a unique $\lambda_{\alpha_m} \mathbf{V}_{\alpha_m} Gm$ of s . We will establish the following conclusion: if T_s has any leading like term in t , then

$$\mathbf{V}_{\alpha_m} Gm = \sum_{j \leq q} \sum_{*} \lambda_{\psi_j} \mathbf{V}_{\psi_j} G_j + \sum_{\phi} \lambda_{\phi} w_{\phi} \mathbf{v}_{\phi}, \quad (4.6)$$

where the $*$ -summation is over all $\mathbf{V}_{\psi_j} G_j$ whose leading term has lower order than that of $\mathbf{V}_{\alpha_m} Gm$. Once (4.6) is established, then we can rewrite f as $\lambda Gq + \tilde{s} + \tilde{t}$, where

$$\tilde{s} = \sum_{j < q} \sum_{\gamma_j} \lambda_{\gamma_j} \mathbf{V}_{\gamma_j} G_j, \quad \tilde{t} = \sum_{\zeta} \lambda_{\zeta} \tilde{h}_{\zeta} \mathbf{v}_{\zeta}, \quad (4.7)$$

such that either $\tilde{s} = 0$, or the leading term of \tilde{s} does not have leading like term in \tilde{t} .

The two observations in Step 2 are also valid in the current situation. The leading term of \tilde{s} can only be cancelled by a term of \tilde{t} , and conversely, the leading term of \tilde{t} can only be cancelled by a term of \tilde{s} . Furthermore, the leading terms of \tilde{s} and \tilde{t} are both non-reduced with respect to G3, Gj for j up to $q-1$. Since the leading term of f is reduced with respect to G3, Gj for j up to $q-1$, it must have higher order than any term of \tilde{s} and \tilde{t} ; then it must be the leading term of Gq , violating the assumption that it is reduced with respect to Gq . This proves that G3, Gj for j up to q is a Gröbner base once (4.6) is true.

Step 8. Once it is proved that G3, Gj for j up to q is a Gröbner base, then for a polynomial f of degree q , by reduction with respect to G3, Gj for j up to $q-1$, we get

that for any term $T = \lambda \mathbf{v}_l \mathbf{V}_{q-2} \mathbf{v}_t$ in the result of reduction, where \mathbf{V}_{q-2} is a monomial of degree $q-2$, the subscripts of $\mathbf{V}_{q-2} \mathbf{v}_t$ and $\mathbf{v}_l \mathbf{V}_{q-2}$ must be both in one of the following normal forms: $Y_1, Y_1 z_1, Y_1 z_1 Y_2, Y_1 z_1 Y_2 z_2, \dots$. If the subscripts of T are not in one of the normal forms, it is easy to show that (1) the subscripts of $\mathbf{V}_{q-2} \mathbf{v}_t$ must be of the form $Y_1 z_1$, and $z_1 = t$; (2) if $Y_1 = h_1 h_2 Y$, where Y is of length $q-4 \geq 1$, then $h_2 > l > h_1$; (3) $h_1 > t$. The only possibility is $\mathbf{v}_l \mathbf{V}_{q-2} \mathbf{v}_t = \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_5 \cdots \mathbf{v}_q \mathbf{v}_1$, the leading term of Gq .

Consider polynomial Gq . By reduction with respect to G3, Gj for j up to $q-1$, we get $Gq = \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_5 \cdots \mathbf{v}_q \mathbf{v}_1 - \mathbf{v}_3 \mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_5 \cdots \mathbf{v}_q \mathbf{v}_2 + g$, where each term of g has leading variable \mathbf{v}_1 or \mathbf{v}_2 . The second term $\mathbf{v}_3 \mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_5 \cdots \mathbf{v}_q \mathbf{v}_2$ and the terms of g are each in a normal form described by the current theorem. Hence, after reduction with respect to the Gq in the above form, each term of f becomes normal.

Step 9. We start to prove (4.6), which is the main part of the whole proof. Let $\mathbf{V}_{\alpha_m} = \mathbf{v}_w \mathbf{V}_{q-m-1}$, and let the leading term of Gm be $\mathbf{V}_{m-1}^G \mathbf{v}_z$, then up to scale $T_s = \mathbf{v}_w \mathbf{V}_{q-m-1} \mathbf{V}_{m-1}^G \mathbf{v}_z$ is the leading term of s , and monomial $\mathbf{V}_{q-m-1} \mathbf{V}_{m-1}^G$ is in normal form, i.e., its subscripts are in one of the forms $Y_1 z_1 \dots Y_k z_k$ and $Y_1 z_1 \dots Y_k z_k Y_{k+1}$. Let l_i, t_i be the leading subscript and trailing subscript of Y_i respectively. Then $l_i \leq t_i$. Let the middle part of Y_i after removing l_i, t_i be C_i .

The tail part of the subscripts $Y_1 z_1 \dots Y_k z_k z$ or $Y_1 z_1 \dots Y_k z_k Y_{k+1} z$ must be either the subscripts $y \tilde{z} z$ from the leading term of G3 for $m=3$, where $y > z$ and $y > \tilde{z}$, or the subscripts $y \tilde{z} Y z$ from the leading term of Gj for $m=j > 3$, where $z \tilde{z} Y$ is ascending. So subscripts $Y_1 z_1 \dots Y_{k-1} z_{k-1} (l_k C_k t_k) z_k z$ where $t_k > z$, belong to the leading term of $\mathbf{V}_{Y_1 \mathbf{v}_{z_1} \dots \mathbf{V}_{Y_{k-1} \mathbf{v}_{z_{k-1}}} \mathbf{v}_{l_k} \mathbf{V}_{C_k} G3$, while subscripts $Y_1 z_1 \dots Y_{k-1} z_{k-1} (l_k C_k t_k) z_k Y_{k+1} z$ where $z_k > z$, belong to the leading term of $\mathbf{V}_{Y_1 \mathbf{v}_{z_1} \dots \mathbf{V}_{Y_{k-1} \mathbf{v}_{z_{k-1}}} \mathbf{v}_{l_k} \mathbf{V}_{C_k} Gj$, where j is the length of Y_{k+1} plus 3. We get

$$\mathbf{V}_{\alpha_m} = \mathbf{v}_w \mathbf{V}_{Y_1 \mathbf{v}_{z_1} \dots \mathbf{V}_{Y_{k-1} \mathbf{v}_{z_{k-1}}} \mathbf{v}_{l_k} \mathbf{V}_{C_k}}. \quad (4.8)$$

If \mathbf{V}_{α_m} is not in normal form, then by reduction with G3, Gj for j up to $q-m$, the order of \mathbf{V}_{α_m} is decreased, and (4.6) is trivially satisfied. Below we assume that \mathbf{V}_{α_m} is normal.

Since T_s has leading like term in t , $\mathbf{v}_w \mathbf{V}_{\alpha_m} \mathbf{v}_{t_k} \mathbf{v}_{z_k}$ for $t_k > z$, and $\mathbf{v}_w \mathbf{V}_{\alpha_m} \mathbf{v}_{t_k} \mathbf{v}_{z_k} \mathbf{V}_{Y_{k+1}}$ for $z_k > z$, must be non-reduced with respect to G3, Gj for j up to $q-1$. It is easy to deduce $k=1$, and when any of the two monomials is non-reduced with respect to G3, the length of Y_1 is less than 3. So up to scale,

$$T_s = \mathbf{v}_w \mathbf{V}_{Y_1 \mathbf{v}_{z_1} \mathbf{v}_z} \text{ or } \mathbf{v}_w \mathbf{V}_{Y_1 \mathbf{v}_{z_1} \mathbf{V}_{Y_2 \mathbf{v}_z}}. \quad (4.9)$$

Only the head part and tail part of T_s are non-reduced with respect to some Gi, Gj respectively, where i, j are between 3 and $q-1$. There are the following cases:

(I) $i = j = 3$. The subscripts of T_s are either $wt_1 z_1 z$ or $wl_1 t_1 z_1 z$, where $w > t_1$ and $t_1 > z$. The first case is considered in Step 3 and is conclusion (4.2). The second case includes six different subscripts of T_s : 51423, 51432, 52413, 52431, 53412, 53421.

(II) $i = 3, j > 3$. The subscripts of T_s are either $wt_1 z_1 Y_2 z$ or $wl_1 t_1 z_1 Y_2 z$, where $w > t_1$ and $z_1 > z$.

(II.1) In the former case, the subscripts of T_s are $w32Y1$, where $w > 3$, and $Y > 3$ is an ascending sequence of length $q-4 > 0$.

(II.2) In the latter case, $t_1 = 4$, and t_1, z_1, z is a permu-

tation of 1,2,3. So T_s has the following possible subscripts: $w143Y2$, $w243Y1$, and $w342Y1$, where $w > 4$, and $Y > 4$ is an ascending sequence of length $q - 5 > 0$.

(III) $i > 3$, $j = 3$. The subscripts of T_s are $wl_1C_1t_1z_1z$, where C_1 is an ascending sequence of length $q - 5 > 0$, $w > l_1 > z_1$ but $w < C_1$, and $t_1 > z$. Obviously $t_1 = q$, but z can take any value from 1 to $q - 1$. So T_s has the following possible subscripts: $4356 \dots q21$, $4356 \dots q12$, $4256 \dots q13$, $3256 \dots q14$, and $3245 \dots \bar{k} \dots q1k$ for $5 \leq k \leq q - 1$. There are the following subcases, considering both the symmetries of the subscripts and the difference of the categories of Gröbner base elements to be used in reduction:

(III.1) The subscripts of T_s are 43521 , 43512 , or 42513 .

(III.2) The subscripts of T_s are $43Y(q-1)q21$, $43Y(q-1)q12$, or $42Y(q-1)q13$, where Y is an ascending sequence of length $q - 6 \geq 0$, and $4 < Y < q - 1$.

(III.3) The subscripts of T_s are 32514 .

(III.4) The subscripts of T_s are $32Yq1(q-1)$, where Y is an ascending sequence of length $q - 5 \geq 0$, and $3 < Y < q - 1$.

(III.5) The subscripts of T_s are $32Y(q-1)q14$, where Y is an ascending sequence of length $q - 6 \geq 0$, and $4 < Y < q - 1$.

(III.6) The subscripts of T_s are $32YZ(q-1)q1k$, where $4 < k < q - 1$, Y is an ascending sequence of length $u > 0$, Z is an ascending sequence of length $q - u - 6 \geq 0$, and $3YkZ(q-1)$ is an ascending sequence.

(IV) $i > 3$, $j > 3$. The subscripts of T_s are $wl_1C_1t_1z_1Y_2z$, where C_1, Y_2 are two ascending sequences of length > 0 , $w > l_1 > z_1 > z$ but $w < C_1$. So $zz_1l_1w = 1234$, and the subscripts of T_s are $43Yk2Z1$, where Y is an ascending sequence of length $u \geq 0$, Z is an ascending sequence of length $q - u - 5 > 0$, and $4YkZ$ is an ascending sequence.

There is no space to present the analyses of all the cases and subcases. We select to present the details for the following representative cases: (I), (II.1), (III.2) to (III.4).

Step 10. The polynomials on the left side of the following equalities are in \mathcal{I}_{j+k}^M : for monomials $\mathbf{V}_j, \mathbf{V}_k$ of degree j, k respectively,

$$\begin{cases} (\mathbf{V}_k + (-1)^k \mathbf{V}_k^\dagger) \mathbf{V}_j - \mathbf{V}_j (\mathbf{V}_k + (-1)^k \mathbf{V}_k^\dagger) = 0, \\ \mathbf{V}_j \mathbf{V}_k - \mathbf{V}_k \mathbf{V}_j - (-1)^{j+k} (\mathbf{V}_j^\dagger \mathbf{V}_k^\dagger - \mathbf{V}_k^\dagger \mathbf{V}_j^\dagger) = 0. \end{cases} \quad (4.10)$$

As long as $j + k < q$, and by applying the above equalities to the leading term of a polynomial f , the order of f is decreased, this transformation of f can always be replaced by reduction with respect to $G3, Gi$ for i up to $j + k$.

Let both $\mathbf{v}_{i_1}, \mathbf{v}_{i_2} \prec \mathbf{v}_{i_3}$ and $\mathbf{v}_{i_1}, \mathbf{v}_{i_2} \prec \mathbf{V}_A$, where A is a sequence of subscripts of length $a < q - 3$. The following order-reducing transformation is also induced by $G3, Gi$ for i up to $a + 3$:

$$\begin{aligned} \mathbf{v}_{i_3} \mathbf{V}_A \mathbf{v}_{i_1} \mathbf{v}_{i_2} &= \mathbf{v}_{i_2} (\mathbf{V}_A \mathbf{v}_{i_1} \mathbf{v}_{i_3} + (-1)^a \mathbf{v}_{i_3} \mathbf{v}_{i_1} \mathbf{V}_A^\dagger) \\ &\quad - (-1)^a \mathbf{v}_{i_1} \mathbf{V}_A^\dagger \mathbf{v}_{i_3} \mathbf{v}_{i_2}. \end{aligned} \quad (4.11)$$

The proof of (4.11) is simple:

$$\begin{aligned} &\mathbf{v}_{i_3} \mathbf{V}_A \mathbf{v}_{i_1} \mathbf{v}_{i_2} \\ &= \mathbf{v}_{i_3} (\mathbf{V}_A \mathbf{v}_{i_1} \mathbf{v}_{i_2} + (-1)^a \mathbf{v}_{i_2} \mathbf{v}_{i_1} \mathbf{V}_A^\dagger) - (-1)^a \mathbf{v}_{i_3} \mathbf{v}_{i_2} \mathbf{v}_{i_1} \mathbf{V}_A^\dagger \\ &= (\mathbf{v}_{i_2} \mathbf{V}_A \mathbf{v}_{i_1} + (-1)^a \mathbf{v}_{i_1} \mathbf{V}_A^\dagger \mathbf{v}_{i_2}) \mathbf{v}_{i_3} + (-1)^a \mathbf{v}_{i_2} \mathbf{v}_{i_3} \mathbf{v}_{i_1} \mathbf{V}_A^\dagger \\ &\quad - (-1)^a \mathbf{v}_{i_1} \mathbf{V}_A^\dagger (\mathbf{v}_{i_3} \mathbf{v}_{i_2} + \mathbf{v}_{i_2} \mathbf{v}_{i_3}) \\ &= \mathbf{v}_{i_2} (\mathbf{V}_A \mathbf{v}_{i_1} \mathbf{v}_{i_3} + (-1)^a \mathbf{v}_{i_3} \mathbf{v}_{i_1} \mathbf{V}_A^\dagger) - (-1)^a \mathbf{v}_{i_1} \mathbf{V}_A^\dagger \mathbf{v}_{i_3} \mathbf{v}_{i_2}. \end{aligned}$$

In later steps, (4.10) and (4.11) are used directly in reduction.

Step 11. Consider case (I) of Step 9. Let $h = \mathbf{v}_5 \mathbf{v}_1 (\mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_3$

$+ \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_3 - \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_2 - \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4)$. Then

$$\begin{aligned} h &= \underline{\mathbf{v}_5 \mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_3} + \underline{\mathbf{v}_5 \mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_3} - \underline{\mathbf{v}_5 \mathbf{v}_1 \mathbf{v}_3} (\mathbf{v}_2 \mathbf{v}_4 + \mathbf{v}_4 \mathbf{v}_2) \\ I_4^M \mathbf{v}_{i, i < 5} &= \underline{-\mathbf{v}_1 \mathbf{v}_5 (\mathbf{v}_4 \mathbf{v}_2 + \mathbf{v}_2 \mathbf{v}_4) \mathbf{v}_3} + \mathbf{v}_4 (\mathbf{v}_5 \mathbf{v}_1 + \mathbf{v}_1 \mathbf{v}_5) \mathbf{v}_2 \mathbf{v}_3 \\ &\quad + \mathbf{v}_2 (\mathbf{v}_5 \mathbf{v}_1 + \mathbf{v}_1 \mathbf{v}_5) \mathbf{v}_4 \mathbf{v}_3 + \underline{\mathbf{v}_1 \mathbf{v}_5 \mathbf{v}_3 (\mathbf{v}_2 \mathbf{v}_4 + \mathbf{v}_4 \mathbf{v}_2)} \\ &\quad - \mathbf{v}_3 (\mathbf{v}_5 \mathbf{v}_1 + \mathbf{v}_1 \mathbf{v}_5) (\mathbf{v}_2 \mathbf{v}_4 + \mathbf{v}_4 \mathbf{v}_2) \\ \mathbf{v}_j I_4^M, j < 5 &= (\mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_3 + \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_3 - \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4 - \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_2) \\ &\quad (\mathbf{v}_5 \mathbf{v}_1 + \mathbf{v}_1 \mathbf{v}_5) \\ I_4^M \mathbf{v}_k &= 0. \end{aligned}$$

When the subscripts 1,2,3 undergo a permutation, the polynomial equalities used in the reduction remain in the same category: $\mathcal{I}_4^M \mathbf{v}_i$ for $i < 5$; $\mathbf{v}_j \mathcal{I}_4^M$ for $j < 4$; $\mathcal{I}_4^M \mathbf{v}_k$. So the above reduction is valid for all the six subcases of Case (I).

Step 12. Case (II.1) of Step 9. Let $h = \mathbf{v}_w (\mathbf{v}_3 \mathbf{v}_2 \mathbf{V}_Y \mathbf{v}_1 + (-1)^q \mathbf{v}_3 \mathbf{v}_1 \mathbf{V}_Y^\dagger \mathbf{v}_2 - (-1)^q \mathbf{v}_1 \mathbf{V}_Y^\dagger \mathbf{v}_2 \mathbf{v}_3 - \mathbf{v}_2 \mathbf{V}_Y \mathbf{v}_1 \mathbf{v}_3)$, where $w > 3$, and $Y > 3$ is an ascending sequence of length $q - 4 > 0$. Then

$$\begin{aligned} h &I_{q-1}^M \mathbf{v}_{i, i < 3} = \underline{-\mathbf{v}_3 \mathbf{v}_w (\mathbf{v}_2 \mathbf{V}_Y \mathbf{v}_1 + (-1)^q \mathbf{v}_1 \mathbf{V}_Y^\dagger \mathbf{v}_2)} \\ &\quad + \mathbf{v}_2 (\mathbf{v}_w \mathbf{v}_3 + \mathbf{v}_3 \mathbf{v}_w) \mathbf{V}_Y \mathbf{v}_1 \\ &\quad + (-1)^q \mathbf{v}_1 (\mathbf{v}_w \mathbf{v}_3 + \mathbf{v}_3 \mathbf{v}_w) \mathbf{V}_Y^\dagger \mathbf{v}_2 \\ &\quad - \mathbf{v}_w (\mathbf{v}_2 \mathbf{V}_Y \mathbf{v}_1 + (-1)^q \mathbf{v}_1 \mathbf{V}_Y^\dagger \mathbf{v}_2) \mathbf{v}_3 \\ \mathbf{v}_j I_{q-1}^M, j < 4 &= \underline{-\mathbf{v}_3 (\mathbf{v}_2 \mathbf{V}_Y \mathbf{v}_1 + (-1)^q \mathbf{v}_1 \mathbf{V}_Y^\dagger \mathbf{v}_2) \mathbf{v}_w} \\ &\quad + (\mathbf{v}_2 \mathbf{V}_Y \mathbf{v}_1 + (-1)^q \mathbf{v}_1 \mathbf{V}_Y^\dagger \mathbf{v}_2) (\mathbf{v}_w \mathbf{v}_3 + \mathbf{v}_3 \mathbf{v}_w) \\ &\quad - \mathbf{v}_w (\mathbf{v}_2 \mathbf{V}_Y \mathbf{v}_1 + (-1)^q \mathbf{v}_1 \mathbf{V}_Y^\dagger \mathbf{v}_2) \mathbf{v}_3 \\ I_{q-1}^M \mathbf{v}_j &= 0. \end{aligned}$$

Step 13. Case (III.2) of Step 9. Let $h = \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} (\mathbf{v}_q \mathbf{v}_2 \mathbf{v}_1 - \mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_q - \mathbf{v}_1 \mathbf{v}_q \mathbf{v}_2 + \mathbf{v}_2 \mathbf{v}_q \mathbf{v}_1)$, where Y is an ascending sequence of length $q - 6 \geq 0$, and $4 < Y < q - 1$. Then

$$\begin{aligned} h &= \underline{\mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_2 \mathbf{v}_1} - \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \underline{\mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_q} \\ &\quad - \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_1 \mathbf{v}_q \mathbf{v}_2 + \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \underline{\mathbf{v}_{q-1} \mathbf{v}_2 \mathbf{v}_q \mathbf{v}_1} \\ &\quad \mathbf{v}_{43Y} \mathbf{G}_4, \\ I_{q-1}^M \mathbf{v}_i &= \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_2 + (-1)^q \mathbf{v}_2 \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3) \mathbf{v}_4 \mathbf{v}_1 \\ &\quad - (-1)^q \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3 \mathbf{v}_1 \\ &\quad - \mathbf{v}_2 (\mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_1 \mathbf{v}_4 + (-1)^q \mathbf{v}_4 \mathbf{v}_1 \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3) \mathbf{v}_q \\ &\quad + (-1)^q \mathbf{v}_1 \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_q \\ &\quad + \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y (\underline{\mathbf{v}_2 \mathbf{v}_q \mathbf{v}_1} - \mathbf{v}_1 \mathbf{v}_q \mathbf{v}_2) \mathbf{v}_{q-1} \\ \mathbf{v}_{42} I_{q-2}^M, I_{q-1}^M \mathbf{v}_i &= \mathbf{v}_2 I_{q-1}^M \mathbf{v}_i \\ &= \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_2 + (-1)^q \mathbf{v}_2 \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3) \mathbf{v}_4 \mathbf{v}_1 \\ &\quad - \mathbf{v}_4 \mathbf{v}_2 (\mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_1 + (-1)^q \mathbf{v}_1 \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3) \\ &\quad + \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_1 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \\ &\quad - \mathbf{v}_2 \mathbf{v}_q (\mathbf{v}_1 \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} + (-1)^q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_1) \\ &\quad + (-1)^q \mathbf{v}_1 \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_q \\ &\quad + (\mathbf{v}_2 \mathbf{v}_q \mathbf{v}_1 - \mathbf{v}_1 \mathbf{v}_q \mathbf{v}_2) \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \\ I_{q-1}^M \mathbf{v}_i, \mathbf{v}_1 I_{q-1}^M &= \underline{\mathbf{v}_1 (\mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_3 - (-1)^q \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger)} \\ &\quad + \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_1 - \mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_1 \\ &\quad + \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_1 (\mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q - (-1)^q \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3) \\ \mathbf{v}_3 I_{q-1}^M, \mathbf{v}_1 I_{q-1}^M &= \underline{\mathbf{v}_1 (\mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_3 - (-1)^q \mathbf{v}_3 \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger)} \\ &\quad - \mathbf{v}_1 (\mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q \mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_3 - (-1)^q \mathbf{v}_3 \mathbf{v}_2 \mathbf{v}_4 \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger) \\ &\quad + \mathbf{v}_2 \mathbf{v}_4 (\mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q - (-1)^q \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3) \mathbf{v}_1 \\ &\quad + \underline{\mathbf{v}_4 \mathbf{v}_2 \mathbf{v}_1} (\mathbf{v}_3 \mathbf{V}_Y \mathbf{v}_{q-1} \mathbf{v}_q - (-1)^q \mathbf{v}_q \mathbf{v}_{q-1} \mathbf{V}_Y^\dagger \mathbf{v}_3) \\ I_{q-1}^M \mathbf{v}_i, \mathbf{v}_1 I_{q-1}^M &= 0. \end{aligned}$$

In the reduction rules, $\mathbf{V}_{43Y}G4$ stands for $\mathbf{v}_4\mathbf{v}_3\mathbf{V}_Y G4$, and so for the rest. The reductions for the other two sub-cases of Case (III.2) are similar.

Step 14. Case (III.3) of Step 9. Let $h = \mathbf{v}_3\mathbf{v}_2(\mathbf{v}_5\mathbf{v}_1\mathbf{v}_4 - \mathbf{v}_4\mathbf{v}_1\mathbf{v}_5 - \mathbf{v}_4\mathbf{v}_5\mathbf{v}_1 + \mathbf{v}_1\mathbf{v}_5\mathbf{v}_4)$. Then

$$\begin{aligned} h &\stackrel{I_4^M \mathbf{v}_i, G5}{=} \mathbf{v}_3\mathbf{v}_1\mathbf{v}_5(\mathbf{v}_2\mathbf{v}_4 + \mathbf{v}_4\mathbf{v}_2) + (\mathbf{v}_2\mathbf{v}_5\mathbf{v}_1 - \mathbf{v}_1\mathbf{v}_5\mathbf{v}_2)\mathbf{v}_3\mathbf{v}_4 \\ &\quad - \mathbf{v}_3\mathbf{v}_1\mathbf{v}_4\mathbf{v}_2\mathbf{v}_5 - (\mathbf{v}_2\mathbf{v}_4\mathbf{v}_1 - \mathbf{v}_1\mathbf{v}_4\mathbf{v}_2)\mathbf{v}_3\mathbf{v}_5 \\ &\quad - \mathbf{v}_2\mathbf{v}_4\mathbf{v}_5\mathbf{v}_1\mathbf{v}_3 - \mathbf{v}_1\mathbf{v}_5\mathbf{v}_4\mathbf{v}_2\mathbf{v}_3 + \mathbf{v}_3\mathbf{v}_2\mathbf{v}_1\mathbf{v}_5\mathbf{v}_4 \\ \mathbf{V}_{31}G3, I_4^M \mathbf{v}_4 &\stackrel{=}{=} \mathbf{v}_3\mathbf{v}_1\mathbf{v}_2\mathbf{v}_4\mathbf{v}_5 - \mathbf{v}_2\mathbf{v}_3\mathbf{v}_1\mathbf{v}_5\mathbf{v}_4 \\ &\quad - \mathbf{v}_1\mathbf{v}_5\mathbf{v}_2\mathbf{v}_3\mathbf{v}_4 + \mathbf{v}_1\mathbf{v}_4\mathbf{v}_2\mathbf{v}_3\mathbf{v}_5 - \mathbf{v}_1\mathbf{v}_5\mathbf{v}_4\mathbf{v}_2\mathbf{v}_3 \\ &\quad + \mathbf{v}_2\mathbf{v}_5\mathbf{v}_1\mathbf{v}_3\mathbf{v}_4 - \mathbf{v}_2\mathbf{v}_4\mathbf{v}_1\mathbf{v}_3\mathbf{v}_5 - \mathbf{v}_2\mathbf{v}_4\mathbf{v}_5\mathbf{v}_1\mathbf{v}_3 \\ &\quad + \mathbf{v}_1(\mathbf{v}_2\mathbf{v}_3 + \mathbf{v}_3\mathbf{v}_2)\mathbf{v}_5\mathbf{v}_4 \\ I_4^M \mathbf{v}_5, \mathbf{v}_1 I_4^M &\stackrel{=}{=} \mathbf{v}_2(\mathbf{v}_1\mathbf{v}_3 + \mathbf{v}_3\mathbf{v}_1)\mathbf{v}_4\mathbf{v}_5 - \mathbf{v}_2\mathbf{v}_4\mathbf{v}_1\mathbf{v}_3\mathbf{v}_5 \\ &\quad + \mathbf{v}_2(\mathbf{v}_5\mathbf{v}_1\mathbf{v}_3 - \mathbf{v}_3\mathbf{v}_1\mathbf{v}_5)\mathbf{v}_4 - \mathbf{v}_2\mathbf{v}_4\mathbf{v}_5\mathbf{v}_1\mathbf{v}_3 \\ \mathbf{v}_2 I_4^M &\stackrel{=}{=} 0. \end{aligned}$$

Step 15. Case (III.4) of Step 9. Let $h = \mathbf{v}_3\mathbf{v}_2\mathbf{V}_Y(\mathbf{v}_q\mathbf{v}_1\mathbf{v}_{q-1} - \mathbf{v}_{q-1}\mathbf{V}_1\mathbf{v}_q - \mathbf{v}_{q-1}\mathbf{v}_q\mathbf{v}_1 + \mathbf{v}_1\mathbf{v}_q\mathbf{v}_{q-1})$, where Y is an ascending sequence of length $q - 5 \geq 0$, and $3 < Y < q - 1$. Then

$$\begin{aligned} h &\stackrel{Gq, I_{q-1}^M \mathbf{v}_i}{=} (\mathbf{v}_2\mathbf{V}_Y\mathbf{v}_q\mathbf{v}_1 + (-1)^q\mathbf{v}_1\mathbf{v}_q\mathbf{V}_Y^\dagger\mathbf{v}_2)\mathbf{v}_3\mathbf{v}_{q-1} \\ &\quad - (-1)^q\mathbf{v}_3\mathbf{v}_1\mathbf{v}_q\mathbf{V}_Y^\dagger\mathbf{v}_2\mathbf{v}_{q-1} \\ &\quad - (\mathbf{v}_2\mathbf{V}_Y\mathbf{v}_{q-1}\mathbf{v}_1 + (-1)^q\mathbf{v}_1\mathbf{v}_{q-1}\mathbf{V}_Y^\dagger\mathbf{v}_2)\mathbf{v}_3\mathbf{v}_q \\ &\quad + (-1)^q\mathbf{v}_3\mathbf{v}_1\mathbf{v}_{q-1}\mathbf{V}_Y^\dagger\mathbf{v}_2\mathbf{v}_q \\ &\quad - (\mathbf{v}_2\mathbf{V}_Y\mathbf{v}_{q-1}\mathbf{v}_q\mathbf{v}_1 - (-1)^q\mathbf{v}_1\mathbf{v}_q\mathbf{v}_{q-1}\mathbf{V}_Y^\dagger\mathbf{v}_2)\mathbf{v}_3 \\ &\quad - (-1)^q\mathbf{v}_3\mathbf{v}_1\mathbf{v}_q\mathbf{v}_{q-1}\mathbf{V}_Y^\dagger\mathbf{v}_2 \\ &\quad + (\mathbf{v}_2\mathbf{V}_Y\mathbf{v}_1 - (-1)^q\mathbf{v}_1\mathbf{V}_Y^\dagger\mathbf{v}_2)\mathbf{v}_3\mathbf{v}_q\mathbf{v}_{q-1} \\ &\quad + (-1)^q\mathbf{v}_3\mathbf{v}_1\mathbf{V}_Y^\dagger\mathbf{v}_2\mathbf{v}_q\mathbf{v}_{q-1} \\ \mathbf{V}_{31}I_{q-2}^M; &\stackrel{\mathbf{v}_i I_{q-1}^M, i < 3}{=} \mathbf{v}_3\mathbf{v}_1\mathbf{V}_Y(\mathbf{v}_q\mathbf{v}_2\mathbf{v}_{q-1} - \mathbf{v}_{q-1}\mathbf{v}_2\mathbf{v}_q - \mathbf{v}_q\mathbf{v}_{q-1}\mathbf{v}_2 \\ &\quad + \mathbf{v}_2\mathbf{v}_q\mathbf{v}_{q-1}) + \mathbf{v}_3\mathbf{v}_1\mathbf{v}_2\mathbf{V}_Y(\mathbf{v}_{q-1}\mathbf{v}_q - \mathbf{v}_q\mathbf{v}_{q-1}) \\ &\quad - \mathbf{v}_2(\mathbf{v}_1\mathbf{v}_3 + \mathbf{v}_3\mathbf{v}_1)\mathbf{V}_Y(\mathbf{v}_{q-1}\mathbf{v}_q - \mathbf{v}_q\mathbf{v}_{q-1}) \\ &\quad + \mathbf{v}_1\mathbf{v}_3\mathbf{v}_2\mathbf{V}_Y(\mathbf{v}_{q-1}\mathbf{v}_q - \mathbf{v}_q\mathbf{v}_{q-1}) \\ \mathbf{V}_{31}I_{q-2}^M, &\stackrel{I_{q-1}^M \mathbf{v}_i}{=} 0. \end{aligned}$$

5. GRÖBNER BASE AND NORMAL FORM FOR VECTOR VARIABLES

THEOREM 8. Let $\mathcal{I}[\mathbf{v}_1, \dots, \mathbf{v}_n]$ be the syzygy ideal of the quaternionic polynomial ring $\mathcal{Q}[\mathbf{v}_1, \dots, \mathbf{v}_n]$ in n vector variables $\mathbf{v}_1 \prec \mathbf{v}_2 \prec \dots \prec \mathbf{v}_n$.

(1) [Gröbner base] The following are a reduced Gröbner base of $\mathcal{I}[\mathbf{v}_1, \dots, \mathbf{v}_n]$: for all $1 \leq i_1 < i_2 < i_3 \leq i_4 \leq \dots \leq i_{m-1} < i_m \leq n$,

VG3:

$$\begin{aligned} [\mathbf{v}_{i_3}\mathbf{v}_{i_2}\mathbf{v}_{i_1}] - [\mathbf{v}_{i_1}\mathbf{v}_{i_3}\mathbf{v}_{i_2}], \quad & [\mathbf{v}_{i_3}\mathbf{v}_{i_1}\mathbf{v}_{i_2}] - [\mathbf{v}_{i_2}\mathbf{v}_{i_3}\mathbf{v}_{i_1}], \\ \mathbf{v}_{i_2}\mathbf{v}_{i_2}\mathbf{v}_{i_1} - \mathbf{v}_{i_1}\mathbf{v}_{i_2}\mathbf{v}_{i_2}, \quad & \mathbf{v}_{i_2}\mathbf{v}_{i_1}\mathbf{v}_{i_1} - \mathbf{v}_{i_1}\mathbf{v}_{i_1}\mathbf{v}_{i_2}; \end{aligned}$$

VGm: $[\mathbf{v}_{i_3}\mathbf{v}_{i_2}\mathbf{V}\mathbf{v}_{i_1}] - [\mathbf{v}_{i_2}\mathbf{V}\mathbf{v}_{i_1}\mathbf{v}_{i_3}]$, where $\mathbf{V} = \mathbf{v}_{i_4}\mathbf{v}_{i_5} \dots \mathbf{v}_{i_m}$, and $m \geq 4$.

(2) [Normal form, see Figure 2] In a normal form, every term is up to coefficient of the form $\mathbf{V}_{Y_1}\mathbf{v}_{h_1}\mathbf{v}_{z_1}\mathbf{V}_{Y_2}\mathbf{v}_{h_2}\mathbf{v}_{z_2} \dots \mathbf{V}_{Y_k}\mathbf{v}_{h_k}\mathbf{v}_{z_k}$ or $\mathbf{V}_{Y_1}\mathbf{v}_{h_1}\mathbf{v}_{z_1} \dots \mathbf{V}_{Y_k}\mathbf{v}_{h_k}\mathbf{v}_{z_k}\mathbf{V}_{Y_{k+1}}$, where (i) $k \geq 0$,

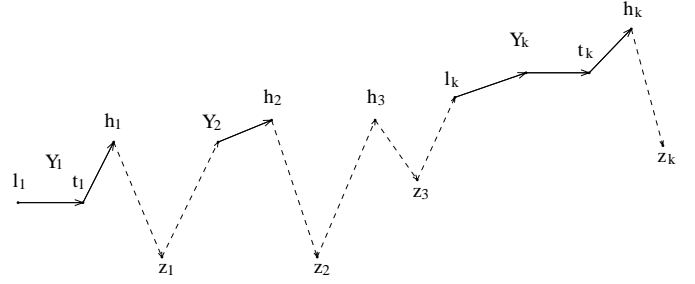


Figure 2: Double-nondescending structure of a quaternionic monomial in normal form, where only the subscripts of vector variables are shown. Each h_i is a peak, while each z_i is a bottom.

- (ii) $\mathbf{v}_{z_1}\mathbf{v}_{z_2} \dots \mathbf{v}_{z_k}$ is non-descending,
- (iii) $\mathbf{v}_{h_1}\mathbf{v}_{h_2} \dots \mathbf{v}_{h_k}$ is non-descending,
- (iv) every \mathbf{V}_{Y_i} is a non-descending monomial of length ≥ 0 ,
- (v) $\mathbf{V}_{Y_1}\mathbf{v}_{h_1}\mathbf{V}_{Y_2}\mathbf{v}_{h_2} \dots \mathbf{V}_{Y_k}\mathbf{v}_{h_k}$ (or $\mathbf{V}_{Y_1}\mathbf{v}_{h_1} \dots \mathbf{V}_{Y_k}\mathbf{v}_{h_k}\mathbf{V}_{Y_{k+1}}$ if $\mathbf{V}_{Y_{k+1}}$ occurs) is non-descending,
- (vi) for every $i \leq k$, $\mathbf{v}_{h_i} \succ \mathbf{v}_{z_i}$,
- (vii) for every $i \leq k$, if the length of \mathbf{V}_{Y_i} is nonzero, let \mathbf{v}_{t_i} be the trailing variable of \mathbf{V}_{Y_i} , then $\mathbf{v}_{t_i} \prec \mathbf{v}_{h_i}$.

Sketch of the proof. Since the generators $V2, V3, V4$ of $\mathcal{I}[\mathbf{v}_1, \dots, \mathbf{v}_n]$ are homogeneous polynomials, if $f \in \mathcal{I}[\mathbf{v}_1, \dots, \mathbf{v}_n]$, then by writing $f = \sum_{\alpha} g_{\alpha}$, where each g_{α} is a homogeneous polynomial, and different g 's have different multisets of variables, we get that each $g_{\alpha} \in \mathcal{I}[\mathbf{v}_1, \dots, \mathbf{v}_n]$. So we simply consider homogeneous polynomials of degree $\leq d$ in r vector variables, where $d \geq r$. Let the multiset of the variables in such polynomials be \mathcal{M} , whose number of elements is d .

The elements of \mathcal{M} are specifications of d different vector variables \mathcal{D} . The definitions of multilinear product and multilinear addition of the multilinear ring for \mathcal{D} are valid for \mathcal{M} after minor revisions. Let $\mathcal{I}^M[\mathcal{M}]$ be the syzygy ideal of the multilinear ring $\mathcal{Q}^M[\mathcal{M}]$ of multilinear polynomials whose variables by counting multiplicity are in multiset \mathcal{M} . We only need to prove the theorem for $\mathcal{I}^M[\mathcal{M}]$.

Most steps of the proof of Theorem 7 are still valid, in particular, (4.6) is valid, whose proof follows a similar classification as in Step 9. Although there are more subtle cases to consider, the reductions for the new situations are much the same as for the cases of Step 9.

6. REFERENCES

- [1] Altman, S.L. *Rotations, Quaternions, and Double Groups*. Oxford University Press, Oxford, 1986.
- [2] Hestenes, D. and Sobczyk, G. *Clifford Algebra to Geometric Calculus*. D. Reidel, Dordrecht, Boston, 1984.
- [3] Li, H. *Invariant Algebras and Geometric Reasoning*. World Scientific, Singapore, 2008.
- [4] Mora, T. An introduction to commutative and noncommutative Gröbner bases. *Theoretical Computer Science* **134** (1994) 131-173.
- [5] Sweedler, M.E. *Hopf Algebra*. Benjamin, New York, 1969.

This paper is supported partially by NSFC 10871195, 60821002/F02, and NCMIS of CAS.